WHAT IS CLAIMED IS:

1. A public key certificate issuing system comprising:

a certificate authority for issuing a public key certificate of an entity which uses said public key certificate; and

a registration authority for sending a public key certificate issuing request received from an entity under control to said certificate authority;

said certificate authority being constituted by a plurality of certificate authorities each executing a different signature algorithm, transferring a public key certificate between said plurality of certificate authorities in response to said public key certificate issuing request received from said registration authority, attaching a digital signature on message data constituting said public key certificate in accordance with said different signature algorithm at each certificate authority, and issuing a multi-signed public key certificate storing a plurality of signatures based on different signature algorithms.

2. The public key certificate issuing system according to claim 1, wherein said plurality of certificate authorities include a Rivest-Shamir-Adleman

certificate authority for executing signature generation processing based on a Rivest-Shamir-Adleman signature algorithm and an elliptic curve cryptography certificate authority for executing signature generation processing based on an elliptic curve cryptography algorithm, said signatures stored in said multi-signed public key certificate including a signature based on said Rivest-Shamir-Adleman signature algorithm and a signature based on said elliptic curve cryptography signature algorithm.

3. The public key certificate issuing system according to claim 1, wherein at least one of said plurality of certificate authorities has a configuration for executing processing of storing a generated signature and signature information including signature algorithm information associated with said generated signature into an extended area of said public key certificate.

4. The public key certificate issuing system according to claim 1, wherein at least one of said plurality of certificate authorities has a configuration for executing processing of storing a generated signature into an area other than a basic area and an extended area of said public key certificate and storing signature information including signature algorithm information associated with said generated signature into said

extended area.

5. The public key certificate issuing system according to claim 1, wherein at least one of said plurality of certificate authorities has a configuration for executing processing of storing, into said public key certificate, flag information indicating whether at least two signatures are included in said public key certificate.

6. A public key certificate issuing method having a certificate authority for issuing a public key certificate of an entity which uses said public key certificate and a registration authority for sending a public key certificate issuing request received from an entity under control to said certificate authority to issue said public key certificate in response to said public key certificate issuing request from said registration authority,

said certificate authority being constituted by a plurality of certificate authorities each executing a different signature algorithm, transferring a public key certificate between said plurality of certificate authorities in response to said public key certificate issuing request received from said registration authority, attaching a digital signature on message data

constituting said public key certificate in accordance with said different signature algorithm at each certificate authority, and issuing a multi-signed public key certificate storing a plurality of signatures based on different signature algorithms.

7. The public key certificate issuing method according to claim 6, wherein at least one of said plurality of certificate authorities executes a step of generating a signature for a signed public key certificate by applying a signature algorithm which is different from that attached to said signed public key certificate and attaching the generated signature to said signed public key certificate.

8. The public key certificate issuing method according to claim 6, wherein

said plurality of certificate authorities include a Rivest-Shamir-Adleman certificate authority for executing signature generation processing based on a Rivest-Shamir-Adleman signature algorithm and an elliptic curve cryptography certificate authority for executing signature generation processing based on an elliptic curve cryptography signature algorithm,

said Rivest-Shamir-Adleman certificate authority executes signature generation processing based on said

Rivest-Shamir-Adleman signature algorithm,

said elliptic curve cryptography certificate authority executes signature generation processing based on said elliptic curve cryptography signature algorithm, and

said multi-signed public key certificate, including a signature based on said Rivest-Shamir-Adleman signature algorithm and a signature based on said elliptic curve cryptography signature algorithm, is issued.

9. The public key certificate issuing method according to claim 6, wherein at least one of said plurality of certificate authorities executes processing of storing a generated signature and signature information including signature algorithm information associated with said generated signature into an extended areas of said public key certificate.

10. The public key certificate issuing method according to claim 6, wherein at least one of said plurality of certificate authorities executes processing of storing a generated signature into an area other than a basic area and an extended area of said public key certificate and storing signature information including signature algorithm information associated with said generated signature into said extended area.

11. The public key certificate issuing method according to claim 6, wherein at least one of said plurality of certificate authorities executes processing of storing, into said public key certificate, flag information indicating whether at least two signatures are included in said public key certificate.

12. An information processing apparatus for executing verification of a public key certificate, having a configuration for selecting, from among a plurality of signature algorithms recorded in signature information stored in a basic area and an extended area of said public key certificate, a signature algorithm which can be verified by said information processing apparatus and executing signature verification on the basis of the selected signature algorithm.

13. An information processing apparatus for executing verification of a public key certificate, comprising a signature verification capability based on a plurality of signature algorithms.

14. The information processing apparatus according to claim 13, wherein said plurality of signature algorithms include a Rivest-Shamir-Adleman signature algorithm and an elliptic curve cryptography signature algorithm.

15. An information recording medium recording a public key certificate storing a public key, said public key certificate storing signatures based on a plurality of signature algorithms.

16. The information recording medium according to claim 15, wherein said plurality of signature algorithms include a Rivest-Shamir-Adleman signature algorithm and an elliptic curve cryptography signature algorithm.

17. A program storage medium for providing a computer program for executing public key certificate issuing processing for issuing a public key certificate of an entity which uses said public key certificate, said computer program comprising the step of generating, with the use of a signature algorithm different from that of a first signature attached to said public key certificate, a second signature and attaching said second signature to said public key certificate.